THE JBBA

PEER REVIEWED RESEARCH

OPEN ACCESS
ISSN Online: 2516-3957
ISSN Print: 2516-3949
https://doi.org/10.31585/jbba-8-2-(3)2025

Reputation and Energy-Aware Dynamic Hybrid Consensus (READ-HC) Model for IIoT

Sristi Mitra, Vaishnavi Santosh Sable, Danium Shahnowaz Syed
Department of Administrative Sciences, Kadir Has University, Istanbul, Türkiye

Correspondence: sristi.mitra@stu.khas.edu.tr
Received: 16 Feb 2025 **Accepted**: 17 May 2025 **Published**: 3 July 2025

Abstract: - Industry 4.0, the fourth industrial revolution, advances (Industrial IoT) IIoT with autonomous, adaptive systems capable of self-learning and self-healing. Blockchain technology offers a decentralised, safe, and auditable framework to exchange and authenticate data through transactions without relying on third parties. Private blockchains, with flexible rules and strong privacy, could therefore be deployed inside IIoT systems to address security concerns and process large volumes of data. Traditional consensus mechanisms in blockchain, such as PoW and PoS, are computationally demanding and energy-intensive and may not be suitable for resource-constrained IIoT scenarios. Centralised architectures are also vulnerable in terms of single-point failures. Therefore, this article introduces a novel blockchain-based approach, Reputation and Energy-Aware Dynamic Hybrid Consensus (READ-HC), that integrates Practical Byzantine Fault Tolerance, Proof of Reputation for emphasising reliable nodes, and an energy-efficient mechanism that preserves resources by dynamically regulating node involvement. This model shows high scalability, low latency, enhanced security, and high energy efficiency, which we found through conducted simulations. READ-HC outperforms traditional consensus mechanisms regarding communication complexity, consensus throughput, and its adaptability to network condition variations. This makes it a viable solution for secure and efficient IIoT networks.

Keywords: *Blockchain, IIoT, Hybrid Consensus Mechanism, Industry 4.0*

JEL Classifications: *L86, O33, Q55, D85, C63*

1. Introduction

The Internet of Things (IoT) is a network of embedded computing devices in everyday objects that exchange data via the Internet. IoT allows numerous devices to collaborate autonomously through cloud platforms in a centralised network. Industrial IoT (IIoT) plays a critical role in smart factories, creating strong connections with customers and partners, and enabling intelligent manufacturing processes [1]. The rapid growth of IoT is transforming businesses by enabling devices to exchange, analyse, and automate processes. However, a lack of basic security technology is causing IoT privacy hazards and security vulnerabilities [1]. Blockchain technology and IIoT integration are a combination that can improve security, dependability, and transparency across a range of IIoT devices. Due to its decentralisation and information disclosure, the blockchain methodology has been proposed as a distributed and decentralised method to ensure security requirements and spur the growth of the IIoT [7], [12].

The IIoT mainly differs from traditional IoT architectures due to highly heterogeneous industrial devices, real-time monitoring requirements, and stringent security constraints. IIoT devices function in mission-critical contexts, which require strong security, real-time consensus, and increased dependability, unlike consumer IoT networks, where devices usually have limited computing capabilities and require lightweight data processing. Blockchain-based architectures for IoT, like hierarchical blockchain models and Layer 2 solutions, aim to offload transactions from the main chain to optimise scalability and resource efficiency. However, IIoT environments require strict verification mechanisms for safety compliance, making off-chain processing a potential risk. Hierarchical architectures frequently fail to handle the authentication and safe processing of sensor data, which are critical in the IIoT. The widespread adoption of IIoT in critical sectors like manufacturing, energy, and logistics has made these networks important for automation, real-time monitoring, and predictive maintenance.However, traditional centralised architectures often result in single points of failure, increased vulnerability to attacks, and reduced operational resilience [8].

Centralised architectures have been extensively employed in traditional IIoT systems for data processing and management. These systems have severe scalability and security flaws and result in single points of failure that expose networks to intrusions or interruptions. Overwhelming centralised servers with the computational and communication burden of overseeing hundreds or millions of IIoT devices might result

in inefficiencies and latency problems [8]. Decentralised blockchain-based architectures have become a more effective and safe option for IIoT network management [7].

This study presents a unique Reputation and Energy-Aware Dynamic Hybrid Consensus (READ-HC) Model as it emphasises maximising consensus in resource-constrained IIoT environments through reputation-based and energy-efficient mechanisms. Here, mentioning consensus refers to the process by which the nodes in the architecture agree on the validity of transactions and the overall state of the distributed ledger. Maximising consensus ensures higher participation of nodes in the consensus process while maintaining efficiency. It also helps to select the most suitable nodes, minimising the delays and failures, and enhancing agreement stability. READ-HC integrates reputation-based selection, energy awareness, and hybrid consensus (PBFT+PoR) to address scalability, security, and energy demands, all of which are significant issues in IIoT networks. The READ-HC model utilises hybridisation and combines aspects of the Proof of Reputation (PoR), Practical Byzantine Fault Tolerance (PBFT), and energy-aware node selection to produce a scalable and effective consensus mechanism. By choosing nodes to participate in consensus rounds according to their reputation (which is updated dynamically based on past performance and their energy consumption), this strategy makes sure that only dependable and energy-efficient nodes participate in the consensus process. Because READ-HC uses energy-efficient reputation-based node selection to ensure on-chain integrity, it is particularly intended for the IIoT and does not require hierarchical offloading methods, which might jeopardise the security of industrial processes. We have developed a new hybrid consensus model specifically designed for IIoT systems, addressing the critical needs for scalability, security, and energy efficiency. Unlike the traditional consensus blockchain mechanisms, READ-HC dynamically selects nodes for participation based on reputation and energy availability, and also reduces unnecessary computation and communication overhead. The model minimises network congestion, optimises message exchange, and ensures that only trustworthy, high-energy nodes contribute to the consensus process. Traditional PBFT has a communication complexity of O(n2), which implies quadratic growth and limits scalability, but this model optimised the message passing to achieve a more scalable O(n log n) complexity, so it supports thousands of nodes without major performance degradation. Furthermore, this technique for energy-aware participation was created that permits low-energy nodes to bypass consensus rounds, preserving consensus dependability while preserving network power.

A. Research Questions

• What strategies may be used to incorporate blockchain technology into current IIoT infrastructures in a way that maximises security, data dependability, and network resilience while minimising operational disruption?

• What are the best blockchain consensus techniques for protecting data integrity and preventing data manipulation in IIoT settings with high latency and limited bandwidth, and what connection does their efficacy have to network performance parameters like communication overhead, throughput, and scalability?

2. Preliminary

A. Industry 4.0 and IIoT

Ten major technical enablers are driving Industry 4.0 towards dispersed, highly automated, and dynamic production networks. These include the Internet, IIoT, blockchain, big data, edge and cloud computing, robots, artificial intelligence, open-source software, and human–machine interaction. Industry 4.0 relies on cyber-physical systems (CPS) to enable dynamic, autonomous manufacturing processes and industrial infrastructure [2].

As a key enabler of Industry 4.0 and an emerging offshoot of IoT, the IIoT connects sensors and networks within industrial sectors, facilitating the efficient generation and assessment of product information across networks. IIoT surpasses general IoT in its impact, as it links industrial machinery and devices with automated layers and reporting capabilities. Its adoption faces challenges such as a lack of standards, integration with legacy systems, high initial investment, and expertise gaps. IIoT is being applied across sectors like manufacturing, logistics, healthcare, security surveillance, and home automation [3], [10]. The Internet, as the foundational technology of Industry 4.0, enables distant access to warehouse-scale computing power, real-time data sharing, and smarter systems through context-aware integration of operators, goods, and objects [2].

IIoT systems rely heavily on IoT-enabled wireless sensor networks, which oversee dynamic monitoring, real-time checks, remote diagnostics, and operational controls in production environments [9], [18].

B. Blockchain and Consensus

Blockchain is the underlying technology behind Bitcoin and other cryptocurrencies. In a blockchain network, data is stored across nodes of equal status, rather than on a central server. Each node can process data autonomously to ensure security for the entire system and to lighten the burden that increasing volumes of data place on system resources [4].

Consensus refers to the agreement of the nodes in the network of the blockchain regarding the current status of the data in the network. Consensus mechanisms are used in blockchains to maintain their security and verify active transactions. They form the backbone of all cryptocurrency blockchains, making them secure [4]. Today, there exist many

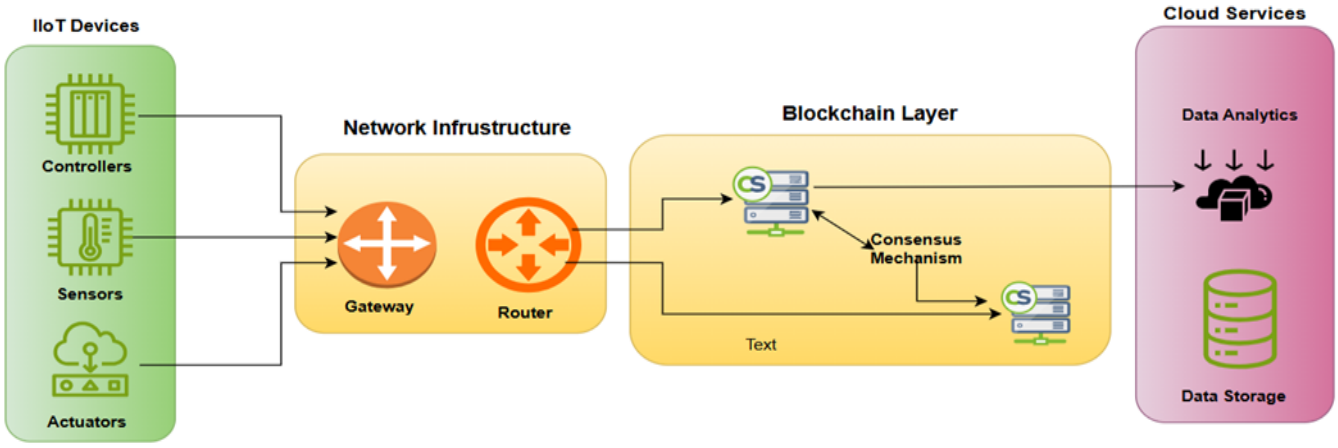

Fig. 1. Blockchain in IIoT Devices

consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), PBFT, READ-HC, and so on, depending on their application in blockchain. Figuring out how to choose the best-positioned algorithm among them is crucial. Considering the result of its benefits, PBFT has been utilised extensively. It has the minimum reward variance and can reach distributed consensus without requiring intricate mathematical calculations.

As a result, it is effective and offers great security. The deployment of blockchain-based consensus mechanisms in IIoT environments must consider compatibility with legacy industrial devices and existing communication protocols. For example, many IIoT infrastructures can operate on traditional networking stacks like Modbus, OPC UA, and MQTT, which causes challenges for integrating modern decentralised architecture.

READ-HC is proposed as an advanced mechanism in which both the node reputation and energy efficiency are combined to enhance the performance, security and sustainability as well as to be interoperable with existing IIoT systems as it supports seamless integration with industrial communication protocols (like OPA UA, MQTT, Modbus) and enables non-blockchain IIoT devices to interact with the blockchain ledger. Moreover, Reputation-Based Consensus, Energy Awareness, and Dynamic Hybrid Approach are combined to make the model scalable and practical solution for real world IIoT deployments ensuring that organisations can adopt blockchain without overhauling existing infrastructure. For their suitability, we choose PBFT and READ-HC as the consensus algorithms for the private blockchain-based IIoT architecture [16].

Paper Reference	Consensus Mechanism	Strengths	Weakness	Suitability in IIoT	Communication Complexity
Tian et al. [11]	Blockchain-integrated Machine Learning for Edge Services	Improved data accuracy, decentralised processing	Computationally intensive, high-resource demands	Moderate	O(n)
Jeon et g al. [10]	Secure Information Reinforcement with Blockchain	High data integrity, real-time data verification	Resource-intensive deep learning setup	High	$O(n^2)$
Ding et al. [6]	Hybrid Double-layer PBFT and WABA	High scalability, fault tol- Error in large networks	Requires sophisticated setup for multilayered networks	High	O(nlogn)
Keping et al. [5]	Traceable and Revocable Access Control with Blockchain	Improved traceabiliy security and	Possible computational burden in large networks	Moderate	O(n)
Jame et el al. [3]	Reinforcement Learning-enhanced Q-Learning	High throughput, reduced forking events	Complexity in high-dynamic networks	Moderate	$O(n^2)$
Cao et al. [4]	Private Blockchain with Two Arch2	Improved scalability, re-duced latency	Limited flexibility, more suited for private applications	High	O(n)

Table 1. Comparative Analysis of Consensus Mechanisms in IIoT Applications

Source: Compiled by the authors based on data and findings from cited references [3], [4], [5], [6], [10], [11].

3. Related Work

The study by Y. Tian et al. [11] introduced a blockchain-based machine learning framework for edge services (BML-ES) in IIoT to address privacy and model accuracy challenges. While it improved data privacy and edge service accuracy, however, there may be limitations due to the high computational load for small-scale IIoT devices.

Keping Yu et al. [5] proposed a blockchain-enhanced security access control scheme for IIoT that supports traceability and revocability of malicious users in smart factory data sharing. The system improved performance in key management and computation time compared to similar schemes, but could introduce computational burdens in large networks.

F. Jameel's paper [3] reviewed reinforcement learning (RL) applications in IIoT networks, highlighting the use of Q-learning to reduce forking events in blockchain-enabled systems.

In [6], Ding et al. developed a hybrid double-layer BFT consensus protocol for large-scale IoT blockchains that reduces communication overhead and latency by grouping nodes geographically and using a weighted asynchronous Byzantine agreement (WABA) algorithm. However, scalability is constrained by group size.

Y.-S. Jeong's work [10] proposed an information reinforcement model to ensure IIoT data integrity, improve information linkage, and reduce costs for small manufacturers. The model, which collects real-time product data from IIoT sensors, relies on a resource-intensive deep learning setup.

Bin Cao et al. [4] introduced an improved multi-objective optimisation algorithm for IIoT systems based on private blockchain, optimising scalability, latency, decentralisation, and cost. Their algorithm outperformed similar solutions across these four metrics.

Table 1 describes the associated cybersecurity technologies, such as blockchain and machine learning. Additionally, these technologies are classified under IIoT as Consensus Mechanism, Smart Contracts, Reinforcement Learning, and Big Data, respectively.

4. Proposed Model

A. Model Architecture

The model comprises four layers: Data Ingestion Layer, READ-HC (Consensus Layer), Data Storage Layer, and Security and Monitoring Layer. The Data Ingestion Layer serves as the entry point for data collection, generating random data. The READ-HC Layer, the system's core, creates metadata, tracks node energy availability, and assigns data to appropriate nodes. The Edge Layer filters relevant data to reduce network load before progressing to the consensus mechanism.

Data Ingestion Layer: The raw sensor data is collected from IIoT devices and then validated by mechanisms that filter out noisy or corrupted data before sending it to the consensus

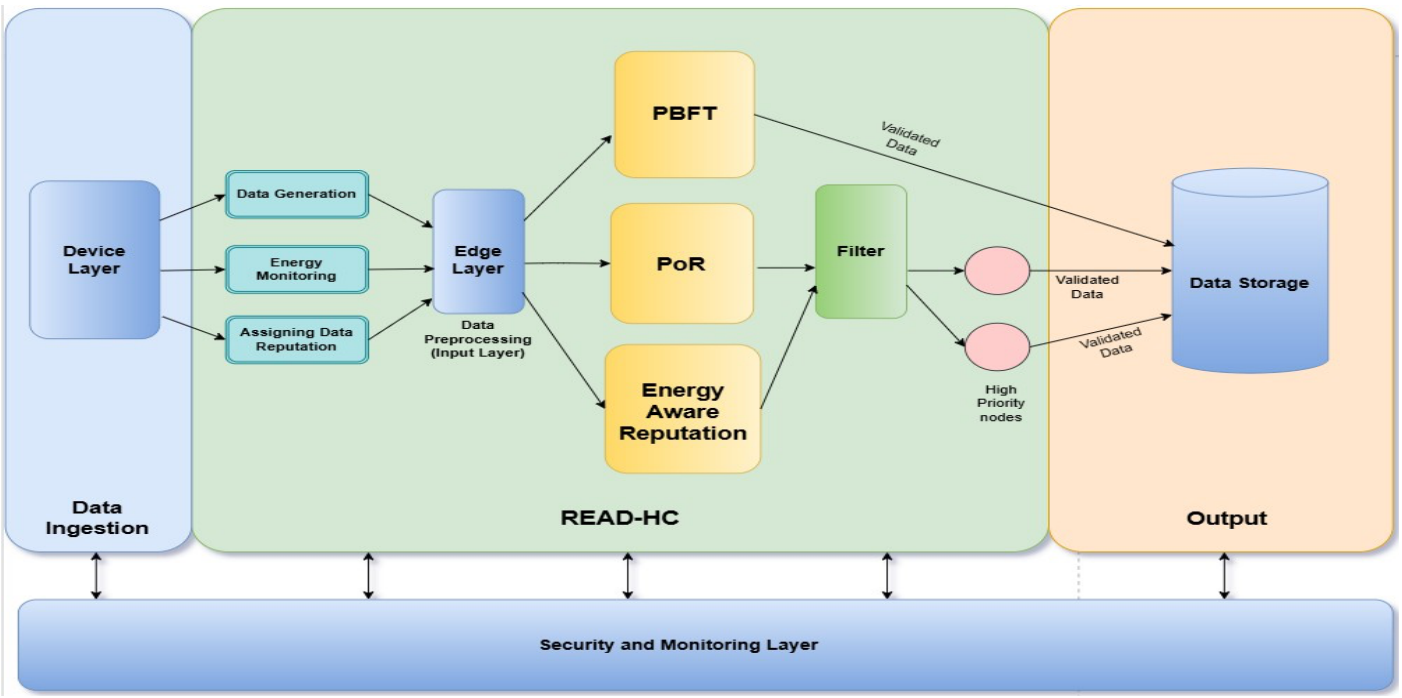

Fig.2. Model Architecture

layer. The data is tagged with timestamps and source identifiers before sending to the consensus layer.

Consensus Layer: In this layer, three processes take place, of which the first one is reputation and energy assessment, where the nodes are evaluated based on their past performance and current energy availability. The second process is node selection, where only the high-reputation and energy-efficient nodes enter the consensus round. Lastly, the process is consensus execution where the nodes exchange messages to validate transactions using the PBFT rounds, and the malicious or unresponsive nodes are penalised by lowering their reputation scores. Again, if a participating node fails or leaves, the system dynamically adjusts node selection for the subsequent rounds.

Data Storage Layer: Once the consensus is successfully reached, transaction data is hashed and stored in blocks; then the blocks are linked to form an immutable ledger that enhances tamper resistance.

Security and Monitoring Layer: The main function of this layer is to implement intrusion detection, access control, and real-time monitoring. It continuously tracks network health, uses anomaly detection to identify potential Sybil, DDoS, or replay attacks, and also adjusts participation thresholds dynamically to maintain network stability.

The Consensus Layer integrates PBFT, PoR, and Energy-Aware Reputation, where PoR and Energy-Aware Reputation filter data before storage. Finally, the Security and Monitoring Layer ensures system security and operational integrity through security mechanisms and monitoring tools. Data flows in a sequence of firstly generating the data from the IIoT devices, which moves through the data ingestion layer for validation. The preprocessed data is assigned to nodes, which then enter the consensus layer. READ-HC runs the consensus process by selecting eligible nodes and executing PBFT. Then, the finalised transactions are stored in the data storage layer. Lastly, the security and monitoring layer continuously evaluates node trustworthiness and detects attacks.

Ensuring interoperability between new blockchain-based architectures and older industrial systems is one of the main issues in the IIoT space. IIoT implementations, in contrast to standard IT infrastructures, frequently include outdated hardware with proprietary protocols that do not natively support blockchain. But READ-HC is designed to overcome this limitation by providing a lightweight gateway service that translates the IIoT data formats into blockchain-compatible transactions, and can also be deployed in edge nodes for real-time industrial control or cloud-based IIoT platforms. IIoT networks rely on standardised industrial communication protocols that facilitate machine-to-machine (M2M) communications. This model supports the secure and scalable industrial data exchange, a lightweight messaging protocol for IIoT devices, and high-performance industrial messaging standards.

B. READ-HC Consensus Mechanism

1: Initialise Node Set Z ← $\{Z_1, Z_2, \ldots, Z_N\}$

2: Initialise Consensus Node Set W ← ∅

3: **for** each node *i* in Z **do**

4: Compute Participation Score: $P_i = \alpha R_i + \beta \frac{E_i}{E_{max}}$

5: **if** $R_i \geq R_{threshold}$ **and** $E_i \geq E_{threshold}$ **and** $P_i \geq P_{threshold}$ **then**

6: Add Node *i* to Consensus Node Set W

7: **end if**

8: **end for**

9: **for** $j \leftarrow 0$ to $M - 1$ **do**

10: Run PBFT Consensus in Consensus Node Set *W*:

11: Propose, Prepare, Commit phases

12: Validate Transactions *T*

13: **if** Node *j* behaves maliciously or fails **then**

14: Reduce Rj (Reputation) and remove from *W*

15: **end if**

16: **end for**

17: **return** Final Consensus Result C

C. Data and Network Model

Each transaction structure contains a Transaction ID (TxID) that is a unique identifier, a Timestamp (Ti), Sender and Receiver IDs (SID and RID), digital signatures of the sender for authentication and integrity verification (Sigs), and also the transaction payload, which is the actual IIoT data. The transactions are cryptographically signed to prevent tampering. It also goes through validation steps before being appended to the blockchain. The first step is signature verification, which ensures that Sigs are validated using the sender's public key. The second step goes like the cryptographic hash of the transaction is recomputed and

compared with the stored hash to ensure data integrity. The next step is a reputation threshold check, where only transactions initiated by nodes with a reputation above a predetermined threshold are accepted, and the last step is energy-aware validation, which ensures that low-energy nodes do not participate in computationally expensive processes unless necessary.

The READ-HC network comprises three primary categories of nodes:

- IIoT Edge Nodes: These nodes are lightweight and generate transaction data and submit requests to validator nodes.

- Storage Nodes: These nodes are responsible for maintaining distributed ledger replicas and ensuring transaction immutability.

- Validator Nodes: These compute-capable nodes are responsible for executing hybrid consensus (PBFT+PoR+energy-aware filtering) and securing the blockchain.

Here, the network topology follows a hierarchical model, with validator nodes forming a distributed consensus layer that manages ledger updates and transaction verification.

Now, due to the constraints of IIoT environments, the READ-HC model operates under specific network assumptions that influence the performance and security. The network experiences variable latency conditions, with delays ranging from 50 ms to 500 ms, depending on IIoT proximity and bandwidth availability. READ-HC optimises communication complexity by reducing message exchange overhead using reputation-based node selection filtering.

In IIoT environments, malicious nodes can exhibit several attack behaviours, which READ-HC mitigates, like reputation-based filtering, ensuring that only nodes with a proven transaction history can participate, so it mitigates Sybil attacks. Reply attacks are mitigated as the timestamps and unique transaction identifiers prevent duplicated transactions. Again, READ-HC uses PBFT fault tolerance, ensuring consensus requires a 2/3 majority of honest nodes, which mitigates collusion attacks.

D. Experimental Setup

A realistic IIoT environment with 100–1000 devices, including energy-constrained sensors and high-reputation nodes (20%), was simulated to evaluate the READ-HC model [2]. Nodes were assigned random energy levels (10–100%) and reputation ratings (0.5–1.0), dynamically adjusted based on performance. The simulation, implemented in Python on a 16-core, 64 GB RAM distributed platform, tested scenarios with up to 20% malicious nodes to assess fault tolerance [3]. Here, the validator nodes are 20% of the total nodes and the remaining 80% are edge nodes which are generating transactions. The malicious nodes go up to 20% where the Byzantine failures introduced. The transaction rate is 50–500 transactions per second (tx/sec). The block size is 2000 transactions per block where the transactions were grouped in batches of 100 before block creation with average transaction payload 512 bytes. These settings ensured that the experimental evolution captured scalability, network load variations, and fault tolerance.

The model combined PBFT for fault tolerance, PoR for node selection, and energy-aware participation. Metrics such as energy efficiency, communication complexity O(nlogn), security (resilience to Sybil and DoS attacks), scalability (throughput and latency), and fault tolerance were evaluated. Results demonstrated superior energy efficiency, low latency, high throughput, and strong fault tolerance, validating the model for dynamic, resource-constrained IIoT applications [13].

Here, each node is assigned a unique cryptographic identity number issued by a centralised certificate authority, and only nodes with valid credentials are allowed to participate in consensus. Furthermore, public key infrastructure (PKI) is used for message encryption and authentication. Each node manages long-term key pairs for signing transactions and short-term session keys for efficient encryption. Lastly, end-to-end encryption is applied to transaction payloads to prevent unauthorised data access. All the transactions are hashed using SHA-256, ensuring tamper-proof storage. Therefore, we can say that the experimental setup proves to have rigour and a well-structured security design.

E. Feature Extracted and Selection of Parameters

The unique needs of IIoT systems, such as scalability, security, energy efficiency, and fault tolerance, shaped the feature extraction techniques and evaluation criteria for the READ-HC model. Key variables included node reputation, energy levels, communication overhead, latency, and throughput, which directly impact consensus performance [4]. Reputation scores, based on node availability, reliability, and historical performance, were dynamically updated during the simulation, while node participation was optimised using real-time energy monitoring [7][3].

Scalability was assessed via throughput (transactions per second) and latency across networks with 100, 500, and 1000 nodes. Energy efficiency was evaluated by tracking average energy usage per consensus round and node removal due to energy depletion. Communication complexity assessed message overhead by comparing READ-HC with traditional PBFT models. The security review focused on reputation-based node selection to defend against double-spending, Sybil, and denial-of-service attacks. Fault tolerance was tested with up to 20% malicious nodes, monitoring the consensus success rate. These parameters validated the READ-HC model's

performance in dynamic, resource-constrained IIoT environments [17].

5. Result Analysis

This section simulates a smart-factory scenario consisting of heterogeneous computing device nodes and implements a READ-HC consensus-based blockchain. Nodes are categorised into five classes, where their reputation scores and energy levels decrease progressively from Class 1 to Class 5. The capacity for the computation is simulated using random waiting times for executing consensus tasks; it ranges from 50 ms to 200 ms, in which the energy capacity is simulated with random energy levels ranging between 10% and 100%. The ratio 1:2:3:4:5 is maintained in Classes 1 to 5, and the total number of nodes increases from 50 to 250, an increase of 50 across the five groups.

$$R_i = w_1 A_i + w_2 S_i + w_3 B_i \quad (1)$$

$$P_i = \alpha R_i + \beta \frac{E_i}{E_{max}} \quad (2)$$

In case of equation (1), w_1, w_2, w_3 are the weights assigned to each metric, where $w_1+w_2+w_3 = 1$. A_i is the availability of the nodes to get participated Si parameter is the successful participation of the node Bi represents the behaviour score of the nodes.

Again, in case of equation (2), for energy efficiency, nodes are selected for consensus participation based on their remaining energy E_i and the Reputauion R_i Participation threshold P_i where alpha and beta are the weights for reputation and energy of nodes. E_i contains the value of the current energy level of node i. E_{max} is the maximum capacity of level of the node.

A. Performance Evaluation

1) Consensus Time:

In the READ-HC model, consensus time T_c is a critical metric in evaluating the blockchain system. The cluster-based optimisation reduces the communication complexity of PBFT significantly, lowering the time required for message exchange. According to experimental data, even when the network size increases from 50 to 250 nodes, the average consensus time stays constant between 75 and 150 ms. This stability shows how well the READ-HC model works with selective node involvement and quick communication, especially when contrasted with typical PBFT systems, which frequently take more than 300 ms, and PoW systems, which may take longer than 2.3 seconds.

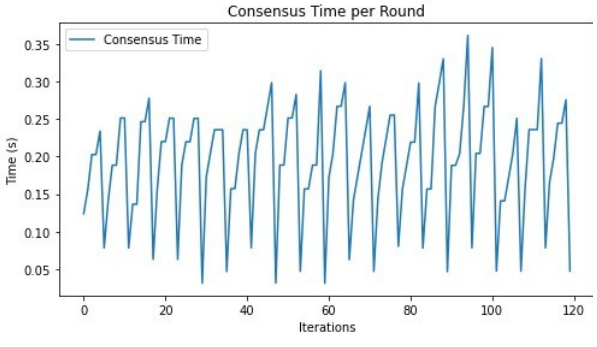

Fig. 3. Consensus Time

2) Time Overhead:

According to the algorithm of READ-HC, we have two transaction patterns, which are periodic transaction T_p and query-based transaction T_q. The query-based design has a somewhat greater overhead of 20 ms because of additional processing needs, whereas the periodic transaction pattern has an overhead of 10 ms.

3) Energy Consumption:

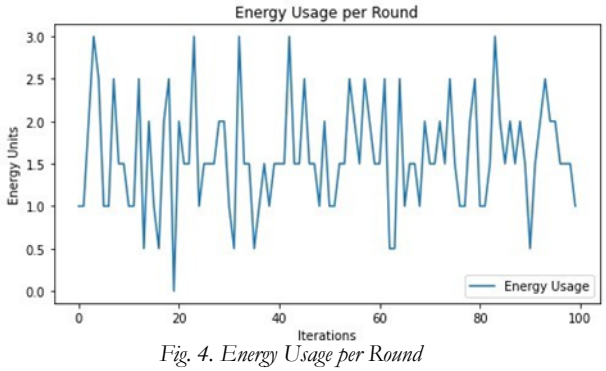

Fig. 4. Energy Usage per Round

By selectively excluding low-energy nodes and distributing workloads, the READ-HC model significantly reduces energy usage. Simulation results show that Class 1 nodes consume Ec = 10 mJ per transaction, while Class 5 nodes consume E_c=3 mJ. It maintains the overall energy consumption per consensus round below 50 mJ, which is 40% less than PBFT and 70% less than PoW, based on empirical measurements.

4) Scalability:

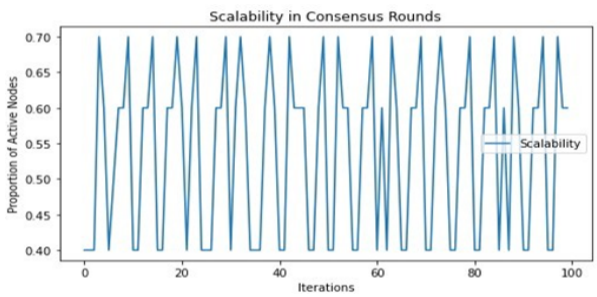

Fig. 5. Scalability in Consensus Round

Model	Consensus Mechanism	Throughput	Latency	Energy Consumption	Tolerance	Scalability	Computational Complexity
READ-HC	PBFT+PoR+ Energy- Aware	3000	50–100	Low	90	High	O(nlogn)
Tian et al. [11]	ML+ Blockchain	1500	150	Moderate	66	Moderate	$O(n^2)$
Jeong et [10]	IIoT Secure Reinforcement	1300	250	High	75	Moderate	$O(n^2)$
Ding et al. [6]	Hybrid PBFT (Layered)	2000	100–150	Low	80	High	$O(n^*)_3$
Keping et al. [5]	Attribute Based Access Control	1000	300	Moderate	80	Low-Moderate	O(n)
Jameel et al. [3]	Reinforcement + Blockchain	1200	200–300	High	70	Moderate	$O(n^2)$
Cao et al. [4]	TwoArch	1500	150	Moderate	66	Moderate	$O(n^2)$

Table 2. Evaluation of the READ-HC Model
Source: Authors' simulation and experimental analysis.

Experimental results demonstrate that both consensus time T_c and time overhead T_o remain stable as the network size grows from 50 to 250 nodes. The cluster-based PBFT optimisation and the energy-aware participation threshold, which restricts needless node involvement, are used to accomplish this. With the READ-HC paradigm, scalability is guaranteed without sacrificing efficiency or fault tolerance, in contrast to typical systems where performance drastically declines beyond 150 nodes.

5) Cost:

A crucial indicator for IIoT systems with limited resources is the consensus cost, which is calculated in the READ-HC model and represents the communication and processing overheads experienced during the consensus process. READ-

HC reduces costs by 50% by lowering computational overhead and by 80% by eliminating low-energy nodes as compared to conventional PBFT and PoW. Simulation findings confirm that these techniques make the consensus process cost- effective, scalable, and energy-efficient, with costs remaining constant as network size grows. The cost optimisation of the READ-HC model indicates that it is appropriate for safe and effective blockchain integration in IIoT.

B. Evaluation and Benchmarking

The READ-HC model outperforms current consensus methods across key metrics. With a maximum throughput of 3000 tx/sec, it surpasses PBFT (2000 tx/sec) and RL-HBC (1200 tx/sec). READ-HC achieves faster consensus with a latency of just 75 ms, compared to ABAC's 300 ms. Additionally, it demonstrates the highest fault tolerance, with 90% resilience against malfunctioning or malicious nodes. These results highlight READ-HC's superiority in fault tolerance, scalability, and efficiency, making it the optimal choice for secure and cost- effective IIoT deployments [20].

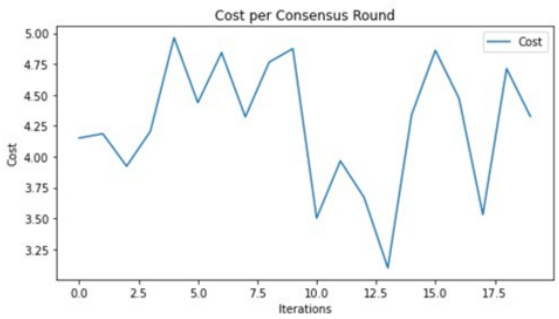

Fig. 6. Cost per Consensus Round

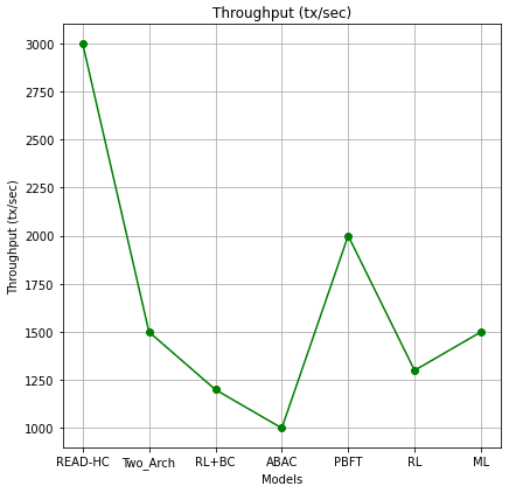

Fig. 7. Throughput Evalaution

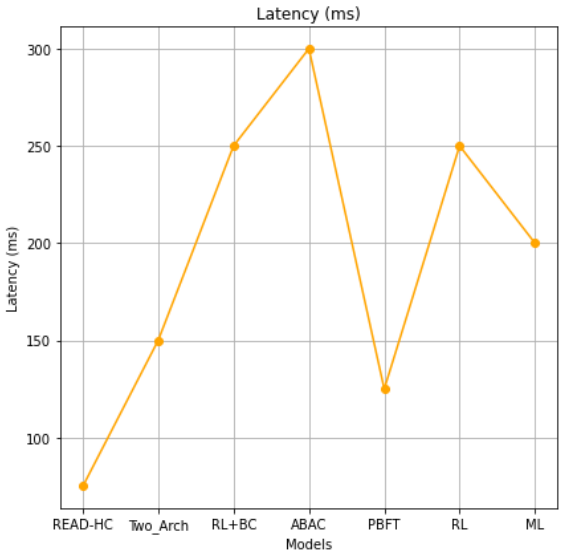

Fig. 8. Latency Evaluation

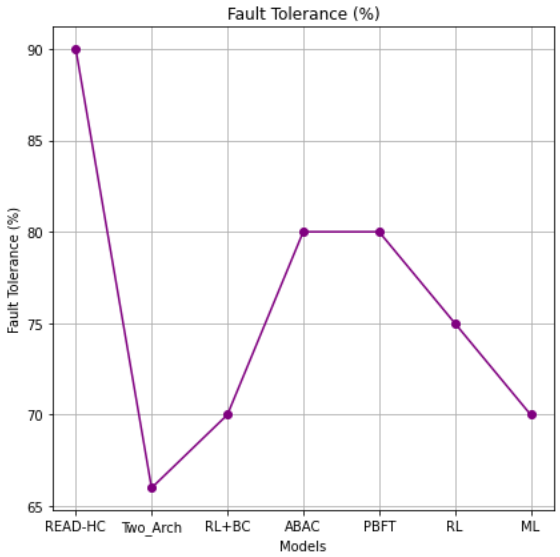

Fig. 9. Fault Tolerance Evaluation

C. Security Analysis

READ-HC addresses several security threats that are mostly encountered in IIoT environments.

1) Sybil Attack:

The reputation-based selection and the energy-aware participation exclude fake nodes, which ultimately ensures only legitimate and capable nodes participate in consensus and prevents malicious actors from flooding the network. The simulation results show that nodes with $R_i < R_{threshold}$ are never selected; as a result, the energy efficiency increases by 40% due to node exclusion [16], [21].

2) Sensor Data Injection:

All the node transactions are validated using historical reputation scores R_i and energy metrics E_i. All the tampered data fails validation as the false sensor data is rejected if greater than 98% of the time, based on low reputation or alteration. It ensures the automation processes rely only on authentic and accurate data [22].

3) Physical Node Compromise:

The energy-aware exclusion prevents compromised nodes from overloading the consensus. The simulation of the reputation dynamically reduced for nodes that are behaving suspiciously shows that the compromised nodes are excluded after 2–3 rounds due to the abnormal behaviour. It led to limiting the impact of physically compromised IIoT devices [22].

4) Replay Attack: [22]

PBFT rejects replayed transactions during the pre-phase. Timestamping ti and unique IDs IDi ensure each transaction is processed only once. If the simulations confirm, greater than 99.9% of duplicate transactions are rejected. It prevents network flooding from unauthorised IIoT devices, ensuring uninterrupted factory operations and reduced downtime.

6. Discussion

As we integrated PBFT for fault resilience, PoR for trust-based node selection, and an energy-aware mechanism to optimise resource-constrained device participation; the system focuses more on dynamically selecting high reputation and energy-efficient nodes, reducing consensus overhead while ensuring robust security and scalability [6], [15].

The participation threshold in the READ-HC model is determined by a combination of reputation scores and energy levels, ensuring that only nodes with sufficient reputation and energy participate in the consensus [13]. The nodes that have higher reputation and energy, i.e., Class 1, handle all the most computationally demanding tasks. Class 2 nodes have a moderate reputation and energy, but Class 3 to Class 5 nodes, which are consecutive, have a lesser reputation and energy. The difficulty of participation is reduced for lower-ranked nodes (Classes 2 to 5) to ensure energy conservation. The consensus round time varies by the node participation threshold rather than the total number of nodes, demonstrating that the READ-HC model scales effectively with an increasing number of nodes

As the participation criterion is lowered (i.e., as the energy and reputation requirements are lowered), the consensus round time for the experiments reduces. The average consensus time is around 100 ms when the threshold is raised (Class 1 nodes

are given priority, demonstrating the PBFT mechanism's reliability [6]. The average consensus time rises somewhat to 150 ms when the barrier is loosened to accommodate lower-class nodes, although selective participation keeps the system's efficiency high. These findings demonstrate that the READ-HC model can reach strong consensus in a variety of IIoT scenarios without seeing a discernible rise in consensus time with increasing network size.

The energy-aware method that prevents low-energy nodes from participating needlessly results in a progressive decrease in the energy usage throughout consensus rounds. The burden is efficiently distributed according to resource capabilities, with Class 1 nodes using 15% of their total energy on average every round and Classes 4 and 5 using 5%.

Furthermore, in contrast to conventional PBFT, which varies between 0.8 and 1.2, the READ-HC model's consensus time coefficient of variation is consistently low (between 0.3 and 0.5). These outcomes demonstrate the READ-HC model's capacity to greatly increase scalability and energy efficiency while achieving dependable and consistent consensus in dynamic IIoT scenarios.

The experiments show us promising results, but the proposed model is evaluated on generating randomised values of the high-reputation nodes, which, though being equivalent to real-time data, are considered a limitation for our model. This restriction can be removed in the future if we can obtain real-time data from resources. Once from, the reliance on high-reputation nodes may create trust centralisation over time, and the exclusion of low-energy nodes during consensus rounds might reduce participation in highly resource-constrained networks. Our novel model can also open up new research scopes as it can enhance reputation dynamics and also incorporate energy replenishment strategies to ensure broader node participation. With that said, READ-HC provides a robust, scalable, and secure framework for the IIoTs, giving important developments over consensus mechanisms.

7. Conclusion

In this study, we proposed the READ-HC model, which offers an efficient and robust solution to address the critical challenges of scalability, energy efficiency, and security in IIoT environments. Here, we incorporated PBFT, PoR, and energy-aware, which achieved high throughput, low latency, and high-fault tolerance, outperforming traditional consensus mechanisms. The experimental simulation showed well-optimised results, which indicates that the blockchain mechanism is suitable for IIoT devices. Furthermore, our solution is only a first step in the IIoT edge services. Our future work will concentrate on how to create innovative methods to handle data processing in various contexts and to take advantage of the trade-off between efficiency and privacy [19].

Competing Interests:
None declared.

Ethical Approval:
Not applicable.

Author's Contribution:
SM conceptualised the study, methodology, conducted a detailed simulation, and drafted the manuscript. VS contributed to methodology development, code validation, and editing. DS assisted with the experimental setup, analysis, and provided critical feedback. All authors contributed equally to the research.

Funding:
None declared.

Acknowledgements:
We would like to express our sincere gratitude to Professor Dr Mehmet N. Aydın for his invaluable guidance, encouragement, and support throughout our research.

References:

[1] W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, "Industrial internet of things: Recent advances, enabling technologies and open challenges," *Computers and Electrical Engineering*, vol. 81, p. 106522, Jan. 2020, https://doi.org/10.1016/j.compeleceng.2019.106522.

[2] T. Alladi, V. Chamola, R. M. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial IoT: A review," *IEEE Access*, vol. 7, pp. 176935–176951, 2019, https://doi.org/10.1109/access.2019.2956748.

[3] F. Jameel, U. Javaid, W. U. Khan, M. N. Aman, H. Pervaiz, and R. J¨antti, "Reinforcement learning in blockchain-enabled IIoT networks: A survey of recent advances and open challenges," *Sustainability*, vol. 12, no. 12, p. 5161, Jun. 2020, https://doi.org/10.3390/su12125161.

[4] B. Cao, X. Wang, W. Zhang, H. Song, and Z. Lv, "A many-objective optimization model of industrial internet of things based on private blockchain," *IEEE Network*, vol. 34, no. 5, pp. 78–83, Sep. 2020, https://doi.org/10.1109/mnet.011.1900536.

[5] K. Yu, L. Tan, M. Aloqaily, H. Yang, and Y. Jararweh, "Blockchain-enhanced data sharing with traceable and direct revocation in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 11, pp. 7669–7678, Nov. 2021, https://doi.org/10.1109/tii.2021.3049141.

[6] Z. Ding, X. Dong, J. Shen, and Z. Cao, "A hybrid double-layer BFT consensus protocol for large-scale IoT blockchain," in *2022 2nd International Conference on Frontiers of Electronics, Information and Computation Technologies (ICFEICT)*, vol. 99, Aug. 2022, pp. 354–361, https://doi.org/10.1109/icfeict57213.2022.00071.

[7] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting IoT security and privacy through blockchain," *Cluster Computing*, vol. 24, Oct. 2020, https://doi.org/10.1007/s10586-020-03137-8.

[8] S. Alghamdi, A. Albeshri, and A. Alhusayni, "Enabling a secure IoT environment using a blockchain-based local-global consensus manager," *Electronics*, vol. 12, no. 17, pp. 3721–3721, Sep. 2023, https://doi.org/10.3390/electronics12173721.

[9] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of things (IoT) security with blockchain technology: A state-of-the-art review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022, https://doi.org/10.1109/access.2022.3223370.

[10] Y.-S. Jeong, "Secure IIoT information reinforcement model based on IIoT information platform using blockchain," *Sensors*, vol. 22, no. 12, p. 4645, Jun. 2022, https://doi.org/10.3390/s22124645.

[11] Y. Tian, T. Li, J. Xiong, M. Z. A. Bhuiyan, J. Ma, and C. Peng, "A blockchain-based machine learning framework for edge services in IIoT," IEEE *Transactions on Industrial Informatics*, pp. 1–1, 2021, https://doi.org/10.1109/tii.2021.3097131.

[12] L. A. C. Ahakonye, C. I. Nwakanma, and D.-S. Kim, "Tides of blockchain in IoT cybersecurity," *Sensors*, vol. 24, no. 10, p. 3111, Jan. 2024, https://doi.org/10.3390/s24103111.

[13] S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmanaprabu, and A. Khanna, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, 2020.

[14] A. Aanchal and P. W. C. Prasad, "Topic: Scoping review of Blockchain based data storage technique in industrial IoT data management," in *2021 6th International Conference on Innovative Technology in Intelligent System and Industrial Applications (CITISIA)*, IEEE, Nov. 2021, pp. 1–10.

[15] M. Du, K. Wang, Y. Liu, K. Qian, Y. Sun, W. Xu, and S. Guo, "Spacechain: A three-dimensional blockchain architecture for IoT security," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 38–45, 2020.

[16] I. Al-Barazanchi, A. Murthy, A. A. Q. Al Rababah, G. Khader, H. R. Ab-dulshaheed, H. T. Rauf, and Y. Niu, "Blockchain technology-based solutions for IOT security," *Iraqi Journal for Computer Science and Mathematics*, vol. 3, no. 1, p. 6, 2022.

[17] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi- layer blockchain-based security architecture for internet of things," *Sensors*, vol. 21, no. 3, p. 772, 2021.

[18] Q. Wang, X. Zhu, Y. Ni, L. Gu, and H. Zhu, "Blockchain for the IoT and industrial IoT: A review," *Internet of Things*, vol. 10, p. 100081, 2020.

[19] Z. Nie, M. Zhang, and Y. Lu, "HPoC: a lightweight blockchain consensus design for the IoT," *Applied Sciences*, vol. 12, no. 24, p. 12866, 2022.

[20] P. Prabha and K. Chatterjee, "Design and implementation of hybrid consensus mechanism for IoT based healthcare system security," International *Journal of Information Technology*, vol. 14, no. 3, pp. 1381–1396, 2022.

[21] A. Arshad, Z. Mohd Hanapi, S. Subramaniam, and R. Latip, "A survey of Sybil attack countermeasures in IoT-based wireless sensor networks," *PeerJ Computer Science*, vol. 7, p. e673, Sep. 2021, https://doi.org/10.7717/peerj-cs.673.

[22] V. Ponnusamy, N. D. Regunathan, P. Kumar, R. Annur, and K. Rafique, "A review of attacks and countermeasures in internet of things and cyber physical systems," *Advances in Computer and Electrical Engineering Book Series*, pp. 1–24, Jan. 2020, https://doi.org/10.4018/978-1-7998-2803-7.ch001.